



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/731,917	12/08/2000	Xin Wang	107146	9895

7590 04/05/2006
Oliff & Berridge PLC
P.O. Box 19928
Alexandria, VA 22320

EXAMINER

NGUYEN, THANH T

ART UNIT PAPER NUMBER

2144

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/731,917

Applicant(s)

WANG, XIN

Examiner

Tammy T. Nguyen

Art Unit

2144

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE (3) MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 January 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

Detailed Office Action

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 20, 2006 has been entered.
2. Claims 1- 13 are presented for examination.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al., (hereinafter Gennaro) U.S. Patent No. 5,937,066 in view of Markus Jakobsson., (hereinafter Jakobsson) U.S. Patent No. 6,687,822.
5. As to claim 1, Gennaro discloses the invention substantially as claimed. Gennaro teaches a method for using a document, comprising: issuing a document usage request for using the document in a session [col.13, lines 47-50], (message transmits is encrypted and decrypted); authenticating the encrypted document (col.10, lines 51-55); receiving authorization to use the encrypted document (col.10, lines 51-55, and col.25, lines 50-60); receiving session key for the session (col.10, lines 58-62); receiving a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key); wherein the session key may be used to decrypt the encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.
6. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].

7. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
8. As to claim 2, Gennaro teaches the invention as claimed, further comprising: retrieving terms and conditions of the session; retrieving usage parameters and system resource information for the session; and comparing the retrieved usage parameters and system resources and the retrieved terms and conditions, wherein the authorized usage is based on comparison results of the retrieved usage parameters and system resources and the retrieved terms and conditions (col.10, lines 51-67).
9. As to claim 3, Gennaro teaches the invention as claimed, wherein the retrieved terms and conditions are associated with at least one of identification of the encrypted document and usage type (col.14, lines 35-38). However, Gennaro does not explicitly disclose partially encrypted.
10. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].

11. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
12. As to claim 4, Gennaro teaches the invention as claimed, wherein the document usage request contains at least one of document identification, usage type, and user identification (col.30, lines 41-55).
13. As to claim 5, Gennaro teaches the invention as claimed, wherein authenticating the protected document comprises at least one of: checking a digital signature associated with the encrypted document; and verifying integrity of each component of the protected document (col.11, lines 30-35). However, Gennaro does not explicitly disclose partially encrypted.
14. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].

15. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jacobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
16. As to claim 6, Gennaro discloses the invention substantially as claimed. Gennaro teaches a usage authorization system for using an encrypted document, comprising: a request receiving device that receives a document usage request for using the encrypted document in a session (col.13, lines 47-50, message transmits is encrypted and decrypted); a document processing device that authenticates the encrypted document (col. 10, lines 51-55); a document source that authorizes usage of the encrypted document, and issues a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key)); an access device that, along with the document device, creates a session key for the session, wherein the session key may be used to decrypt the partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.

17. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
18. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
19. As to claim 7, Gennaro teaches the invention as claimed, wherein the document source retrieves terms and conditions of the session, retrieves usage parameters and system resource information for the session, and compares the retrieved usage parameters and system resources and the retrieved terms and conditions, the authorized usage being based on comparison results of the retrieved usage parameters and system resources and the retrieved terms and conditions (col.10, lines 51-67).
20. As to claim 8, Gennaro teaches the invention as claimed, wherein the retrieved terms and conditions are associated with at least one of identification of the encrypted

document and usage type (col. 14, lines 35-38). However, Gennaro does not explicitly disclose partially encrypted.

21. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
22. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
23. As to claim 9, Gennaro teaches the invention as claimed, wherein the document usage request contain at least one of document identification, usage type, and user identification (col.30, lines 41-55).
24. As to claim 10, Gennaro teaches the invention as claimed, wherein the document processing device authenticates the protected document by at least one of: checking a digital signature associated with the encrypted document; and verifying integrity of each component of the encrypted document (col.11, lines 30-35). However, Gennaro does not explicitly disclose partially encrypted.

25. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
26. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
27. As to claim 11, Gennaro teach the invention as claimed, comprise a combination of performing partial rendering transformation (col.5, lines 45-65).
28. As to claim 12, Gennaro teaches the invention as claimed, wherein the session and proxy keys are not usable for directly decrypting the encrypted document without rendering the encrypted document and performing proxy transformation on the rendered document (16, lines 45-50). However, Gennaro does not explicitly disclose partially encrypted.
29. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted

- (Jakobsson teaches each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
30. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.
31. As to claim 13, Gennaro discloses the invention substantially as claimed. Gennaro teaches a method for using a partially encrypted document, comprising: receiving a document usage request for using the encrypted document in a session [col.13, lines 47-50]; authorizing use the encrypted document (col.10, lines 51-55); creating a session key for the session, and issuing a proxy key that delegates decryption to the session (col.10, lines 57-67, key encrypting key allowing them to decrypt the encrypted data keys (session key), wherein the session key enable: rendering a non-encrypted portion of the partially encrypted document; performing a proxy transformation on the partially rendered, partially encrypted document(col.10, lines 51-55, and col.25, lines 50-60); and decrypting the proxy transformed, partially rendered, partially encrypted document using the session key, wherein the session key may be used to decrypted the a partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted

- document are available to an end user. However, Gennaro does not explicitly disclose partially encrypted and proxy key.
32. In the same field of endeavor, Jakobsson discloses (e.g., a method and system for providing translation certificates). Jakobsson discloses partially encrypted and proxy key (Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption). [see Jakobsson, col.6, lines 19-27 and col.10, lines 1-16].
33. Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Jakobsson's teaching of a method and system for providing translation certificates with the teachings of Gennaro to have a partially encrypted and proxy key because it would have provided specific techniques to provide for the secure and controlled electronic distribution of documents across a communications network, such as internet.

Response to Arguments

34. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments include the failure of previously applied art to expressly disclose partially encrypted and proxy key (see Applicant's response, Dated January 20, 2006, Page 7). It is evident from the detailed mappings found in the above rejection(s) that Gennaro and Jakobsson disclosed this functionality (see Jakobsson teaches the proxy has the key that allow to decrypt the transcript, each server performs on partial decryption and one partially encryption).

Art Unit: 2144

[see Jackobsson, col.6, lines 19-27 and col.10, lines 1-16). Further, it is clear from the numerous teachings (previously and currently cited) that the provision for proxy key and partially encrypted was widely implemented in the networking art. Thus, Applicant's arguments drawn toward distinction of the claimed invention and the prior art teachings on this point are not considered persuasive.

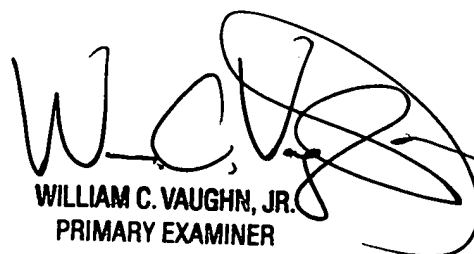
Conclusion

35. Any inquiries concerning this communication or earlier communications from the examiner should be directed to **Tammy T. Nguyen** who may be reached via telephone at (571) 272-3929. The examiner can normally be reached Monday through Friday between 8:00 a.m. and 5:00 p.m. eastern standard time.

If you need to send the Examiner, a facsimile transmission regarding this instant application, please send it to (703) 872-9306. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's Supervisor, **VAUGHN JR WILLIAM**, may be reached at (571) 272-3922.

TTN

March 30, 2006



WILLIAM C. VAUGHN, JR.
PRIMARY EXAMINER